EPO - Munich
88

18. Mai 2007

CONFIRMATION

Notice of Opposition to a European Patent

To the
European Patent Office

Tabulation marks

for EPO use only

I. Patent opposed

Opp. No. OPPO (1)

Patent No. EP 0974129

Application No. 96932173.6

Date of mention of the grant in the European Patent Bulletin (Art. 97(4), 99(1) EPC) 16 August 2006

Title of the invention: Trusted infrastructure support systems, methods and techniques for secure electronic commerce, electronic transactions, commerce process control and automation, distributed computing, and rights management

II. Proprietor of the Patent

first named in the patent specification Intertrust Technologies Corp.

Opponent's or representative's reference (max. 15 spaces) OREF

III. Opponent

OPPO (2)

Name: F.R. Kelly & Co

Address:
27 Clyde Road,
Ballsbridge,
Dublin 4, Ireland

State of residence or of principal place of business: IE

Telephone/Telex/Fax:

Multiple opponents: ☐ further opponents see additional sheet

IV. Authorisation

1. Representative
(Name only one representative to whom notification is to be made)

OPPO (9)

Name: Wallace, Alan

Address of place of business:
F.R. Kelly & Co.
4 Mount Charles,
Belfast,
BT7 1NZ, United Kingdom

Zur Kasse

Telephone/Telex/Fax: +44 28 9023 6000 +44 28 9023 5454

Additional representative(s): ☒ (on additional sheet/see authorisation) OPPO (5)

2. Employee(s) of the opponent authorised for these opposition proceedings under Art. 133(3) EPC

Name(s):

Authorisation(s)

☒ not considered necessary

☐ has/have been registered under No.

☐ is/are enclosed

To 1./2.

for EPO use only

V. Opposition is filed against

— the patent as a whole ☒

— claim(s) No(s).

VI. Grounds for opposition:

Opposition is based on the following grounds:

(a) the subject-matter of the European patent opposed is not patentable (Art. 100(a) EPC) because:

— it is not new (Art. 52(1); 54 EPC) ☒

— it does not involve an inventive step (Art. 52(1); 56 EPC) ☒

— patentability is excluded on other grounds, i. e. Art. 52(2) ☒

(b) the patent opposed does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art (Art. 100(b) EPC; see Art. 83 EPC). ☒

(c) the subject-matter of the patent opposed extends beyond the content of the application/ of the earlier application as filed (Art. 100(c) EPC, see Art. 123(2) EPC). ☒

VII. Facts and arguments

(Rule 55(c) EPC)
presented in support of the opposition are submitted herewith on a separate sheet (annex 1) ☒

VIII. Other requests:

See Annex 1

IX. Evidence presented

for EPO use only

Enclosed = ☐

will be filed at a later date = ☒

A. **Publications:** — Publication date

1 WO 9624092

Particular relevance (page, column, line, fig.): See Annex 1

2 EP 0715247

Particular relevance (page, column, line, fig.): See Annex 1

3

Particular relevance (page, column, line, fig.):

4

Particular relevance (page, column, line, fig.):

5

Particular relevance (page, column, line, fig.):

6

Particular relevance (page, column, line, fig.):

7

Particular relevance (page, column, line, fig.):

Continued on additional sheet ☐

B. **Other evidence**

See Annex 1

Continued on additional sheet ☐

X. Payment of the opposition fee is made

for EPO use only

☒ as indicated in the enclosed voucher for payment of fees and costs (EPO Form 1010)

☐

XI. List of documents

Enclosure No.		No. of copies		for EPO use only
0	☒ Form for notice of opposition	2	(min. 2)	
1	☒ Facts and arguments (see VII.)	2	(min. 2)	
2	Copies of documents presented as evidence (see IX.)			
2a	☐ — Publications		(min. 2 of each)	
2b	☐ — Other documents		(min. 2 of each)	
3	☐ Signed authorisation(s) (see IV.)			
4	☒ Voucher for payment of fees and costs (see X.)	1		
5	☐ Cheque			
6	☒ Additional sheet(s)	2	(min. 2 of each)	
7	☒ Other (please specify here): Form 1037	1		

XII. Signature of opponent or representative

Alan Wallace, Professional Representative

Place Belfast

Date 16 May 2007

Please type name under signature. In the case of legal persons, the position which the person signing holds within the company should also be typed.

ANNEX 1

Opposition against: European Patent Number: EP-B-0974129
Application Number: 96932173.6
Date of grant: 16th August 2006

Name of Proprietor: Intertrust Technologies Corp.

Title of the invention: Trusted Infrastructure support systems, methods and techniques for secure electronic commerce, electronic transactions, commerce process control and automation, distributed computing, and rights management

Name of Opponent: F.R. Kelly & Co
Address of Opponent: 27 Clyde Road, Dublin 4, Ireland

State of residence of Opponent: Ireland

Re Box VII: Indication of the facts, evidence and arguments

1. Added Matter

The subject-matter of the patent extends beyond the content of the application as filed (A100(c)).

The subject-matter of the patent, and particularly the claims, has an information content that differs from the information content of the application as filed.

Claim 1

Claim 1 is based upon a claim filed as the Primary Request before Oral proceedings, and then amended for patentability reasons at the Oral proceedings.

1.1 Original claim 1 was directed to using 'distributed' clearing operations. This is no longer a feature of the claim as granted. Subject matter has been added.

1.2 The proprietor in its letter of 22nd February 2006 states:

Added Subject Matter Art 123(2) EPC
Primary Request
In the first paragraph of the annex to the summons to oral proceedings the Examining division notes that the claims as originally filed include reference to a clearing operation and that removal of this feature would extend the content of the application as originally filed. In view of this, claim 1 of the primary request is based on claim 1 of the PCT application as originally filed. The apparatus claim originally filed has been amended to recite a method of using the apparatus and apparatus features present in the original claim 1 have been retained.

The latter part of original claim 1 included features relating to a clearing operation. Looking at former claim 7, it can be seen that the clearing operation could include performing at least one rights management task. Claim 1 as filed herewith includes steps which satisfy this limitation and thus claims a specific clearance operation. Basis for the step of sending a request to access digital content from the user's appliance may be found on page 259, lines 8 to 10. Basis for the step of receiving at the user's appliance digital content from the second appliance may be found on page 250 lines 10 to 13. Basis for the step of receiving from a certifying authority a digital certificate attesting to at least one attribute of the user may be found on page 261 lines 1 and 2. Basis for the feature that

use of the received content is dependent upon receipt of an appropriate digital certificate may be found on page 261 lines 21 to 23.

It is submitted that, as claim 1 of the main request claims a method for accessing digital content using an electronic commerce and/or rights management apparatus including steps of a clearing operation, no subject matter has been added in contravention of Art 123(2) EPC. In particular, it is noted that the claim has not been broadened and that claim 1 of the main request falls entirely within the scope of originally filed claim 7.

The proprietor incorrectly asserts that granted claim 1 includes steps that satisfy the limitations of original claim 1 in combination with original dependent claim 7.

However, in claim 1 as granted:
a) there is no disclosure of any distributed clearing operation cf. original claim 1.
b) the following features present in original claims 1 and 7 are absent from granted claim 1:

- the system is for performing at least one clearing operation (original claim 1)
- the first electronic appliance performs at least a first part of the clearing operation (original claim 1)
- the second electronic appliance performs at least a second part of the clearing operation (original claim 1)
- the first part of the clearing operation comprises at least one rights management task (claim 7)

c) Claim 7 does not support the proprietor's assertion that a rights management task is a particular example of a clearing operation. Original claim 1 recites that a clearing operation has two (distributed) parts. Original claim 7 recites that one of these parts may comprise a rights management task.

d) The proprietors assertion that the scope of granted claim 1 is entirely within the scope of original claim 7 is incorrect. For example, original claim 7 recited that the system performs a clearing operation in two parts at different appliances but granted claim 1 does not recite this. Original claim 7 recited that a first part of the clearing operation performed at the first appliance comprises at least one rights management task but granted claim 1 does not recite this. Original claim 1 has a scope including that the second appliance does not perform a rights management task (see original claim 8) but granted claim 1 does not.

1.3 There is no disclosure in the application as originally filed of the following features recited in claim 1:
a) "sending a request to access digital content to the second appliance (100)"- the application as filed instead discloses, at page 259 lines 9 to 10, sending "an electronic message to provider 168 requesting the specific information they want to receive".
b) "receiving at the user's appliance digital content from the second appliance (100)"- the application as filed instead discloses, at page 259 lines 10 to 13, that "provider 168 may deliver this information 166 within VDE secure electronic containers 152 along with associated rules and controls 188 that control pricing and permissions".
c) "a digital certificate attesting to at least one attribute of the user"- the application as filed instead discloses, at page 261, lines 1 to 3, that "a certifying authority 500 may deliver digital certificates to each of consumers 95 specifying a consumer's one or more classes"
d) "wherein the rule and control define a use of received content"- the application as filed instead discloses, at page 261, line 21 to page 262, line 2, that "Control set 188(1) may, for example, contain a requirement that the consumer 95(1) must have a certificate 504(1) from an independent certifying authority 500 (or from information distributor or other party acting in a certifying capacity under authorization from a more senior certifying authority) attesting to the fact that the consumer 95(1) has a subscription that has not yet expires to the online encyclopedia."

Claim 1 therefore has an information content that extends beyond the information content of the application as filed. The generalized features recited in the claims are not disclosed in the application text and add subject matter. Also arbitrary selection of features from combinations of features recited in the description adds subject matter.

Claim 2

Claim 2 would appear to be based on claim 5 as originally filed. However, original claim 5 recited that there is a first part of a (distributed) clearing operation and that the first part comprises a usage metering task. Granted claim 2 does not recite this feature. Matter has been added.

Claim 3

There is no disclosure in the claims as filed or the application as filed of performing a micro-payment aggregation task at a user's appliance. There is merely a disclosure that micro-payment aggregation can be distributed. There is no disclosure of how it is distributed. there is no disclosure that it may be performed by a single user appliance or that it can be performed by the user appliance that receives digital content and a digital certificate.

It is noted that some features described above, which constitute 'added matter', are technical features. Their removal from the claim is therefore impermissible during the Opposition proceedings (A 123(3)) as such removal would extend the protection conferred.

2. Sufficiency

The patent does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art (A100(b)).

For example, in relation to the invention defined by claim 1:

2.1. The claim recites a "protected processing environment" but the patent does not describe how to make or obtain a protected processing environment.

2.2. A feature or features presented as essential for a solution to the problem solved by the invention, is/are not present in the claim. The claim therefore does not represent a workable invention as it is missing an essential feature. For example, the claim is missing the essential feature of a 'distributed' clearing operation.

2.3. The features identified in section 1 (added subject matter) are not disclosed in the application as filed nor is it disclosed how to implement them.

Consequently, the European patent application does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.

3. Patentability

Filing Date: 4th September 1996
Priority Date: None

Documents and Evidence it is intended to rely upon (Prior Art)

O1. WO9624092 published 8th August 1996
O2. EP0715247 published 5th June 1996

All documents cited in the International search report, the European search report, during examination of the European application and during examination of other equivalent applications for the invention whether in Europe or elsewhere.

Evidence of the common general knowledge at the effective filing date of the invention. In particular, evidence concerning the existence and use of digital certificates for attesting to an attribute of a user.

The opponent indicates its intention to rely on additional facts, evidence and arguments should the claims be amended to introduce as yet unclaimed technical features.

The claims

The subject-matter of the European patent is not patentable within the terms of Articles 52 to 57. Each of claims 1 to 3 lacks novelty and/or inventive step in view of the prior art when taken as a whole.

The invention as defined by the various claims is not new and/or does not involve an inventive step.

Document O1

Claim 1	**WO9624092 published 8th August 1996**
A method for accessing digital content using an electronic commerce and/or rights management apparatus, the apparatus comprising	
a user's electronic appliance (100)	"The user's data processor, which is shown in Fig. 13 ... It comprises ...a memory 26 and a network adapter 27...the memory 26 also stores a user program 35 and, preferably, a database 36 intended for the control data. Depending upon the current operation, a data package 40 can be stored in the memory 26...The user program 35 controls the usage of a data object in accordance with the control data, which is included in the data package together with the data object."
having a protected processing environment (154)	"When the user has finished usage of the data object, the user program 35 restores the data package in the secure form by repackaging it, step 1518." "It is important to mention that the user

	program 35 never stores the object in native format in user accessible storage and that during display of the data object the print screen key is trapped."
a second electronic appliance (100'), and	"The data provider's data processor (Fig 2)... the data object provider may be an author of a data object, an owner of a data object, a broker of a data object or anyone else who wants to distribute a data object, while retaining the control of its usage."
an electronic communications network (150) that allows the user's and second appliances (100, 100') to exchange digital signals	"...the data package which may now be distributed by file transfer over a network, or on storage media such as CD ROM or diskette, or by some other means." ... "The file transfer program 1409 can transfer and receive files via network to and from other data processor."
wherein the method comprises the steps of: sending a request to access the digital content from the user's appliance (100) to the second appliance (100')	"When a user wants to use a data object, he contacts the broker and requests authorization for usage of the data object."
receiving at the user's appliance (100) digital content from the second appliance	"First the user receives a data package 40 via file transfer over a network, or on a storage media such as CD-ROM or diskette, or by any other appropriate means, step 1501"
and an associated rule and control (188)	"The data object may also be packaged as a consequence of a request from a user for usage of the data object. In that case the package may include control data which is specifically adapted to that user. This control data is called a user set of control data." "The general set of control data comprises at least one or more usage control elements, which define usages of the data object which comply with the predetermined conditions. These usages may encompass for instance the kind of user, a time limit for usage, a geographical area for usage, allowed operations, such as making a hard copy of the data object or viewing it, and/or claim to royalty payment. The general set of control data may comprise other kinds of control elements besides the usage control element. In a preferred embodiment, the general set of control data comprises a security control

	element which defines a security procedure which has to be carried out before usage of the data object."
receiving at the user's appliance (100) from a certifying authority (500) a digital certificate attesting to at least, one attribute of the user,	"The user program 35 can have code which controls use of the program by password or by any other suitable method. A password may be added in a password control element during packaging of the data object. The password is transferred to the user by registered mail or in any other appropriate way. In response to the presence of the password control element in the control data structure, the user program prompts the user to input the password." .... "When the data package is sent to the user, the public key is mailed to the user by registered mail. When the user program is executed in response to a request for usage of this data object, the usage manager module will detect the security module code in the control data and call the security module. This module passes control to the user interface module 1402, which requests the user to input the public key. If the key is correct, the user security module applies complementary decryption using that key and passes a usage approved message to the usage manager module, which enables the usage." ... *The attribute attested to is the user's identity*
wherein the rule and control define (188) defines a use of the received content	"The usage manager module 1403 then compares the user request for usage with the corresponding control data, steps 1506-1507. If the requested usage is not permitted in the control data, the requested usage is disabled, step 1508. However, if the requested usage is approved of in the control data, the usage manager module 1403 applies any format and security modules 1406, 1407 specified in the header data or usage data, steps 1509-1514, to the data package."
which use is dependent upon receipt of an appropriate digital certificate,	The user program 35 can have code which controls use of the program by password or by any other suitable method. A password may be added in a password control element during packaging of the data object. The password is transferred to the user by registered mail or in any other appropriate way. In response to the presence of the password control element in the control data structure, the user program prompts the user to input the password.

	.... When the data package is sent to the user, the public key is mailed to the user by registered mail. When the user program is executed in response to a request for usage of this data object, the usage manager module will detect the security module code in the control data and call the security module. This module passes control to the user interface module 1402, which requests the user to input the public key. If the key is correct, the user security module applies complementary decryption using that key and passes a usage approved message to the usage manager module, which enables the usage.
and the protected processing environment (154) enforces the rule and control (188)	The usage manager module 1403 then compares the user request for usage with the corresponding control data, steps 1506-1507. If the requested usage is not permitted in the control data, the requested usage is disabled, step 1508. However, if the requested usage is approved of in the control data, the usage manager module 1403 applies any format and security modules 1406, 1407 specified in the header data or usage data, steps 1509-1514, to the data package.

The invention as defined by claim 1 is not new and/or does not involve an inventive step in view of O1.

Claim 2	
A method according to claim 1 further comprising the step of metering usage of the digital content at the user's appliance.	"The artist wants to provide a free preview of the image, but also wants to be paid on a per use basis" The claim is obvious as some form of metering is required if payment is to be on a per use basis.

The invention as defined by claim 2 is not new and/or does not involve an inventive step in view of O1.

Claim 3

Claim 3 is merely a common design variant. It is common practice to aggregate 'small' tasks until they become a 'large' task.

The invention as defined by claim 3 is not new and/or does not involve an inventive step in view of O1.

Document O2

Claim 1	**EP0715247 published 5th June 1996**
A method for accessing digital content using an electronic commerce and/or rights management apparatus, the apparatus comprising	see below
a user's electronic appliance (100)	Rendering Repository/System
having a protected processing environment (154)	It should be noted that the dashed line defining printer system 401 defines a secure system boundary. Communications within the boundary are assumed to be secure. Depending on the security level, the boundary also represents a barrier intended to provide physical integrity... The printer repository 402 is an instantiation of the rendering repository 205 of Figure 2. Figure 4b is an example of a computer system as a rendering system. ...The dashed box surrounding the computer system 410 represents a security boundary within which communications are assumed to be secure. The display/execution repository 411 is further coupled to a credit server 414 to report any fees to be billed for access to a digital work and a repository 415 for accessing digital works stored therein.
a second electronic appliance (100'), and	Repository 1
an electronic communications network (150) that allows the user's and second appliances (100, 100') to exchange digital signals	When transactions occur between more than one repository, it is assumed that there is a reliable communication channel between the repositories. For example, this could be a TCP/IP channel
wherein the method comprises the steps of: sending a request to access the digital content from the user's appliance (100) to the second appliance (100')	The digital work remains securely in Repository 1 until a request for access is received. The request for access begins with a session initiation by another repository. Here a Repository 2 initiates a session with Repository 1, step 103. As will be described in greater detail below, this session initiation includes steps which helps to insure that the respective repositories are trustworthy.

receiving at the user's appliance (100) digital content from the second appliance	a creator creates a digital work, step 101. The creator will then determine appropriate usage rights and fees, attach them to the digital work, and store them in Repository 1, step 102. When a sending repository transmits a message to a receiving repository, the sending repository encrypts all of its data using the public writing key of the receiving repository. In this way, the communication can only be read (to a high probability) by the receiving repository, which holds the private checking key for decryption.
and an associated rule and control (188)	The term "usage rights" or "rights" is a term which refers to rights granted to a recipient of a digital work. Generally, these rights define how a digital work can be used and if it can be further distributed. Each usage right may have one or more specified conditions which must be satisfied before the right may be exercised.
receiving at the user's appliance (100) from a certifying authority (500) a digital certificate attesting to at least, one attribute of the user,	The respective public keys for the repositories to be used for encryption are obtained in the registration transaction described below.
wherein the rule and control define (188) defines a use of the received content	The term "usage rights" or "rights" is a term which refers to rights granted to a recipient of a digital work. Generally, these rights define how a digital work can be used and if it can be further distributed. Each usage right may have one or more specified conditions which must be satisfied before the right may be exercised.
which use is dependent upon receipt of an appropriate digital certificate,	Communication with an authorization repository 202 may occur when a digital work being accessed has a condition requiring an authorization. Conceptually, an authorization is a digital certificate such that possession of the certificate is required to gain access to the digital work.... An authorization may be required by both repositories involved in an access to a digital work. A usage transaction is carried out in a session between repositories. For usage transactions involving more than one repository, or for financial transactions between a repository and a credit server, a registration transaction is performed.

	The steps described are from the perspective of a "repository-1" registering its identity with a "repository-2". The registration must be symmetrical so the same set of steps will be repeated for repository-2 registering its identity with repository-1...Referring to Figure 16, repository-1 ...then generates a registration message, step 1602. A registration message is comprised of ...the identification certificate for the repository-1...The identification certificate is encrypted by the master repository in its private key and attests to the fact that the repository (here repository-1) is a bona fide repository... Repository-1 then transmits the registration message to repository-2, step 1603...Upon receiving the registration message, repository-2 determines if it has the needed public key for the master repository, step 1604...If repository-2 does not have the needed public key to decrypt the identification certificate, the registration transaction terminates in an error, step 1618. ..Assuming that repository-2 has the proper public key the identification certificate is decrypted, step 1605..... When a sending repository transmits a message to a receiving repository, the sending repository encrypts all of its data using the public writing key of the receiving repository. In this way, the communication can only be read (to a high probability) by the receiving repository, which holds the private checking key for decryption ...
and the protected processing environment (154) enforces the rule and control (188)	The term "usage rights" or "rights" is a term which refers to rights granted to a recipient of a digital work. Generally, these rights define how a digital work can be used and if it can be further distributed. Each usage right may have one or more specified conditions which must be satisfied before the right may be exercised.

The invention as defined by claim 1 is not new and/or does not involve an inventive step in view of O2 or the combination of O1 and O2.

Claim 2	**EP0715247 published 5th June 1996**
A method according to claim 1 further comprising the step of metering usage of the digital content at the user's appliance.	"The simplest model, used by conventional software, is that there is a single fee at the time of purchase, after which the purchaser obtains unlimited rights to use the work as often and for as long as he or she wants. Alternative models, include metered use and variable fees. The grammar differentiates between uses where the charge is per use from those where it is metered by the time unit. "

The invention as defined by claim 2 is not new and/or does not involve an inventive step in view of O2 or the combination of O1 and O2.

Claim 3	**EP0715247 published 5th June 1996**
A method according to claim 1 further comprising the step of performing at least one micro-payment aggregation task at the user's appliance.	"The credit server 301 is a device which accumulates billing information for the repository 201. The credit server 301 communicates with repository 201 via billing transactions 302 to record billing transactions. Billing transactions are reported to a billing clearinghouse 303 by the credit server 301 on a periodic basis." "Preferably, the credit server would store the fee transactions and periodically communicate via a network with the billing clearinghouse for reconciliation." "Thus, a single device can be both a repository and a credit server, provided that it has the appropriate processing elements for carrying out the corresponding functions and protocols."

The invention as defined by claim 3 is not new and/or does not involve an inventive step in view of O2 or the combination of O1 and O2.